REMARKS

Applicants have now had an opportunity to carefully consider the Examiner's comments set forth in the Office Action of November 2, 2004.

Reconsideration of the Application is requested.

The Office Action

Claims 1-48 were presented for examination.

The disclosure was objected to because of Informalities. Specifically, correction of "FIGS. 2-5" to –FIGS.2-6– on page 5, line 4 was required by the Examiner.

Claim 8 stands rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Further, the Examiner noted that claim 8 recites the limitation "the step of creating a client session" in line 1 without sufficient antecedent basis.

Claims 1-37 and 41-44 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,668,322 issued to Wood et al. (hereinafter Wood).

Claims 38-40 and 45-48 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wood in view of U.S. Patent No. 6,785,704 issued to McCanne.

Objections

The paragraph on page 5, lines 4-5, has been amended as requested by the Examiner, thereby changing "FIGS. 2-5" to –FIGS.2-6–. Further, other paragraphs in the specification, although not objected to by the Examiner, have been amended to correct minor inadvertent typographical errors.

For the foregoing reasons, the specification should now be in proper form for examination.

Non-art Rejections

Regarding the 35 U.S.C. § 112, second paragraph, rejection of dependent claim 8, the recited limitation of "the step of creating a client session" in line 1 is no longer present in the claim as a result of the above-listed amendments to the claims.

For the reason stated above, dependent claim 8 should now satisfy the requirements set forth in 35 U.S.C. § 112, second paragraph.

Art Rejections

In rejecting claims 1-37 and 41-44 under 35 U.S.C. § 102(e), the Office Action made reference to col. 7, lines 1-18 of Wood as anticipating the step of "creating a challenge at the originating server" as recited in claim 1. Applicants respectfully traverse the Examiner's opinion with regard to the teachings of Wood. The challenge, as recited in claim 1, is a challenge generated at the server. For example, page 11, lines 1-17, of the present application teach that "the web server 20 creates a unique, random string called a challenge (step 204). The actual string of the challenge preferably includes at least three parts: a unique alpha numeric prefix, a non-alpha numeric delimiter character, and a sequence of random bytes. The random bytes may be generated in any of a number of methods." It is clear from the recited claim limitation and the detailed description that the challenge is created at the web server in response to receiving a communication from a client.

Wood, on the other hand, teaches that login credentials are obtained from a principal (e.g., a human user) via a browser client as evidence that the principal is entitled to a particular entity. The specific login credentials may include, e.g., a password, a certificate, results of a biometric process, results of an Enigma challenge or results of a smart card interrogation. But, in all of these cases, the credentials are known and provided by the browser client, and not created on the web server.

The created challenge recited in claim 1 of the present application is used, for example, during redirects of the client browser from the web server to the central sign-on server (page 11, lines 18-21) and during redirects from the central sign-on server to the web server (page 12, lines 12-16). An association is maintained between the session created for the client browser and the created challenge as long as the client browser keeps the session current (page 13, lines 1-3). Further, the challenge is used for looking up session records by the central server (page 17, lines 19-20).

The server-created challenge, as disclosed by the present application, and recited in claim 1, is fundamentally different than the logon credentials taught by Wood. The logon credentials of Wood correspond to the log-in identification of the present application, however, the client browser of the present application only provides log-in identification after the central sign-on server has determined that it

does not yet recognize a session for the client browser. That is to say, the client browser is asked to provide authentication information only after the randomly created challenge string is not recognized, as described on page 12, lines 4-6, 12-14, and 17-23. This challenge string concept is neither taught nor suggested by the cited reference.

Claim 1, as amended, includes a limitation on the originating server belonging to a federation of trusted servers. Support for this limitation is found in the abstract and numerous places in the specification, and is described in more detail starting on page 8, line 16. Claim 1, as amended, further includes a limitation wherein client authentication is received from the client using the browser only if no session is present in the federation of servers for the client, otherwise receiving the authenticating information from the central sign-on server. Support for this limitation is shown with respect to step 308 in FIG. 3, and described in detail starting on page 14, line 20.

The concepts of the limitations, as recited in the subject claim, as amended, are neither taught nor suggested by the cited reference. For example, Wood describes a single sign-on only for applications and/or resources (190) accessible to a Gatekeeper (110 in Fig. 1). A user "interacts with enterprise applications and/or resources 190 and the security architecture via a gatekeeper/entry handler component 110 and a login component 120" (col. 9, lines 19-22). Wood does not teach a user or browser having direct access to the resources (190) without interacting with the gatekeeper (110). On the other hand, the present application describes a federation of servers using a centralized sign-on system that would be more transparent to the user. For example, the user is not required to access a server by means of a Gatekeeper, but, as is customary, connects to the desired server, and the centralized sign-on process occurs transparently to the user as recited in claim 1, as amended.

For the reasons stated above, it is respectfully submitted that independent claim 1, as amended, and claims 2-8 and 10-11, depending therefrom, are patentably distinct over the cited reference, and in condition for allowance.

Independent claim 12 has been amended herein to recite limitations similar to those in claim 1. Specifically the encrypted communication received by the central sign-on server includes a server-created challenge string, and the web server is a member of a federation of trusted servers, and the client is recognized based on a previously initiated session on at least one of the trusted servers.

The above-listed limitations of claim 12, as amended, are neither taught nor suggested by Wood. Applicants therefore submit that independent claim 12 and claims 13-25, depending therefrom, are patentably distinct over the cited reference, and in condition for allowance.

Independent claim 26, as amended, recites a limitation for "running a session freshening task for sessions on each web server of a plurality of web servers, each web server comprising a trusted server included in a federation of trusted servers, each trusted server trusting the remaining trusted servers in the federation" which, as discussed above, is neither taught nor suggested by Wood. There is no suggestion that the resources (190) comprise a federation of trusted servers. Further, claim 26, as amended, recites a limitation wherein an encrypted communication sent by the web server to the central sign-on server includes a web-server-created challenge string. This limitation also is neither taught nor suggested by Wood.

For the reasons cited above, Applicants submit that independent claim 26 and claims 27-31, depending therefrom, are patentably distinct over the cited reference, and in condition for allowance.

Independent claim 32, as amended, is a method for session maintenance dealing particularly with session termination aspects of the session maintenance. The subject claim includes a limitation for "recognizing a client on a web server, the web server belonging to at least one federation of trusted web servers, each trusted web server trusting the remaining web servers in the federation." As discussed above, Wood neither teaches nor suggests a federation of trusted web servers. The subject claim also includes limitations for terminating a local session for the client on a second trusted web server based on an encrypted communication from the first web server to the central sign-on server. This concept also is neither taught nor suggested in the cited reference. Nor is the limitation with reference to the web-server-created challenge string taught or suggested by Wood.

For the reasons cited above, Applicants submit that independent claim 32 and claims 33-40, depending therefrom, are patentably distinct over the cited reference, and in condition for allowance.

Independent claim 41, as amended, is directed to a system configured to implement the methods of claims 1, 12, 26, and 32. As amended, the claim includes a limitation for "a plurality of servers, each server configured to communicate with at

least one client, each server being a member of at least one federation of trusted servers, each trusted server trusting the remaining servers in the federation." Again, as discussed above, Wood neither teaches nor suggests a federation of trusted web servers. Further, the central sign-on server is configured to receive a server-created challenge string from the communicating server which is also neither taught nor suggested by Wood.

For the reasons cited above, Applicants submit that independent claim 41 and claims 42-48, depending therefrom, are patentably distinct over the cited reference and in condition for allowance.

With reference to dependent claims 38-40 and 45-48. Applicants respectfully traverse the opinion stated in the Office Action that McCanne teaches sending the encrypted message to each web server for which the central sign-on server has a record of an active session associated with the client (with reference to FIG.6, numeral 54). The servers 40 in the server array are not servers to which a client connects for access to to a resource in the same sense as in Wood or the present application. Rather, the servers 40 are simply used in a content distribution system "to receive requests and get broadcast content delivered to individual clients" (col. 12, lines 30-31). That is to say, "the content reaches server array 54 over distribution network 52. Because distribution network 52 is arranged as a network, the content can be scaleably distributed to many servers in server array 54" (col. 12, lines 43-46). The client would have no knowledge of these servers, or that content was being distributed over them, being aware only of the servers (14) to which the client (12) is connected (col. 8, lines 37-38). Thus, the client would not have any active sessions on these servers.

For the above-stated reasons, Applicants submit that McCanne does not teach or suggest a federation of trusted servers on each of which a client may establish a session, but rather, only a network of servers for scalably distributing content to the client, and that McCanne, therefore, cannot be suitably combined with Wood to arrive at the limitations of dependent claims 38-40 and 45-48, as amended. Nor is there any suggestion that combining McCanne with Wood would arrive at features of the present application as recited in the subject dependent claims.

CONCLUSION

For the reasons detailed above, it is respectfully submitted all claims remaining in the application (Claims 1-8 and 10-48) are now in condition for allowance.

In the event the Examiner considers personal contact advantageous to the disposition of this case, he/she is hereby authorized to telephone Steven M. Haas, at (216) 363-9149.

Respectfully submitted,

FAY, SHARPE, FAGAN,
MINNICH & McKEE, LLP

April 4, 2005
Date

Steven M. Haas
Reg. No. 37,841
1100 Superior Avenue
7th Floor
Cleveland, Ohio 44114-2579
(216) 861-5582

Certificate of Mailing

Under 37 C.F.R. § 1.8, I certify that this Amendment is being

☒ deposited with the United States Postal Service as First Class mail, addressed to: MAIL STOP AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

☐ transmitted via facsimile in accordance with 37 C.F.R. § 1.8 on the date indicated below.

☐ deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. 1.10 on the date indicated below and is addressed to: MAIL STOP AMENDMENT, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Express Mail Label No.:	Signature
Date	**Printed Name**
April 4, 2005	**Steven M. Haas**

N:\PATC\200007\GTY0000278V001.doc